sorensoncommunications™

4393 South Riverboat Rd, Ste 300
Salt Lake City, UT 84123
T 801.287.9400
F 801.287.9401
W www.sorenson.com

February 23, 2007

Via Electronic Filing

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123
Written Ex Parte Communication

Dear Ms. Dortch:

Sorenson Communications, Inc. ("Sorenson") urges the Federal Communications Commission ("FCC") to take immediate action to ensure that providers are able to combat IP Relay fraud. IP Relay has proven to be of great benefit to deaf and hard-of-hearing individuals, enhancing their quality of life by providing a superior alternative to traditional text telephone ("TTY") devices. As Sorenson and others have explained, however, the usefulness of IP Relay has been threatened by fraudulent misuse of the service. Of particular concern are IP Relay calls from people located outside the United States who place calls to U.S. merchants and use stolen or fake credit cards to order merchandise and have it shipped overseas.

Unless the Commission acts to address this problem, merchants will become less willing to accept IP Relay calls, and, as a result, deaf and hard-of-hearing Americans will no longer be able to rely on IP Relay as a means of conducting important transactions in their day-to-day lives. It is imperative that the Commission take immediate action to protect American businesses and consumers from fraud and to preserve IP Relay for deaf and hard-of-hearing users.

In the past year, Sorenson adopted procedures to prevent fraudulent IP Relay calls. These procedures have proven very effective and Sorenson believes that misuse of IP Relay has declined significantly as a result of its actions. Although it would be counter-productive to disclose the specific actions Sorenson has taken to deter fraud,[1]

---

[1] *See* Comments of Sorenson Communications, Inc. at 7 (July 3, 2006) ("Sorenson IP Fraud Comments") (explaining that making the fraud-detection criteria public would give the perpetrators of fraud a roadmap of how to circumvent the criteria). (Unless otherwise indicated, all comments and *ex parte* filings cited herein were filed in CG Docket No. 03-123.)

Sorenson notes that it has not received a single complaint from a user claiming that he or she was prevented from making a legitimate IP Relay call.

Sorenson's experience demonstrates that IP Relay fraud can be prevented effectively with minimal effect on legitimate IP Relay users. Accordingly, Sorenson urges the FCC to authorize and encourage providers to adopt procedures for identifying and preventing fraudulent and harassing IP Relay calls. The comments filed in the *IP Fraud Proceeding* suggest a number of anti-fraud measures that providers may take, including:

- Blocking all international calls;
- Undertaking a systematic program for educating merchants about the fraud problem, and developing some "best practices" they can adopt (*e.g.*, asking for a security number on credit cards);
- Allowing communications assistants to terminate harassing calls from hearing or non-hearing individuals;
- Recording the IP address or other identifying information of a caller who has placed fraudulent calls in the past and using such information to identify or monitor future calls; and
- Developing criteria for identifying fraudulent calls, and notifying the called party (*e.g.*, a merchant) during the call and asking if the call should be terminated.[2]

The development of criteria for identifying fraudulent calls is likely to be one of the most useful tools for providers seeking to prevent such calls. For example, it is likely that only a very small number of legitimate IP Relay calls involve credit card transactions. In fact, Sorenson believes that forty percent or more of the IP Relay calls relayed by Sorenson before it proactively implemented its new fraud-prevention procedures involved a credit card. Tellingly, that number has dropped to less than 2 percent of all calls since Sorenson's anti-fraud measures took effect.[3] Because some deaf and hard-of-hearing users can be expected to make IP Relay calls that involve the use of credit cards, it would be imprudent to prohibit the use of credit cards during IP Relay

---

[2] *See, e.g.*, Sorenson IP Fraud Comments at 5-14; Comments of AT&T Inc. at 3-4 (July 3, 2006); Comments of Telecommunications for the Deaf and Hard of Hearing, Inc., *et al.*, at 8-9 & n.5 (July 3, 2006); *Ex Parte* Comments of Nordia, Inc. at 1-5 (Sept. 7, 2006); Comments of Sprint Nextel Corporation at 3-7 (July 3, 2006); Comments of Verizon at 7-9 (July 3, 2006).

[3] As noted above, this reduction in credit card calls appears to be solely due to a reduction in fraudulent calls, as there is no indication that legitimate IP Relay calls have been affected in any way.

calls. Nonetheless, if credit cards are rarely used for legitimate calls but frequently used for fraudulent calls, this information may be used to prevent fraud, as described below.

First, the Commission should clarify that providers are authorized to implement all of the safeguards described above, including the use of criteria, such as credit card transactions, for identifying fraudulent calls.

Second, the Commission should require providers to monitor and report the percentage of IP Relay calls that involve the use of a credit card. To protect users' privacy, providers would track and report credit card usage only in the aggregate and would not identify the particular calls in which credit cards were used. Such aggregate information, such as a spike in the percentage of calls using credit cards, would serve as a red flag for providers and the FCC, and suggest the need for additional examination and perhaps additional actions. Because there are clearly legitimate IP Relay calls that involve the use of credit cards, the FCC should also clarify that providers are not permitted to notify the called party and ask if the call should be terminated based solely on the fact that the call involves the use of a credit card.

In addition, the Commission should make clear that providers are entitled to compensation for any conversation minutes they relay before a call is identified as fraudulent.

Finally, Sorenson notes that there does not appear to be any reason to implement similar anti-fraud procedures for video relay service ("VRS"). As the leading provider of VRS, Sorenson is very sensitive to the potential misuse of that service. However, while Sorenson remains vigilant for signs of VRS-based fraud, it has not seen any evidence of such misuse to-date, and does not reasonably expect to see such misuse in the future. In Sorenson's view, there are a number of factors making VRS an unlikely target for fraud. Unlike IP Relay, for example, VRS users must be fluent in ASL. In addition, VRS lacks the anonymity of IP Relay, as the user's face appears on the screen. Furthermore, the vast majority of Sorenson VRS users apply for Sorenson videophones and have Sorenson install those devices in the user's home. As a result, VRS is much less susceptible to fraud than IP Relay. Accordingly, there is no need for providers or the FCC to take any action to deter VRS fraud.

This letter is being submitted for inclusion in the record of the above-referenced proceeding, in accordance with the Commission's rules.

Sincerely,

/s/ Michael D. Maddix

cc: Cathy Seidel
Jay Keithley
Thomas Chandler
Gregory Hlibok